



9 in 10 Enterprises Report Gaps Between the Cybersecurity Culture They Have and the One They Want

New research from ISACA and the CMMI Institute finds that few employees understand their role in protecting information (Sydney, Australia (16 October 2018)—With cybersecurity threats continuing to escalate worldwide, the ISACA/CMMI Institute Cybersecurity Culture Report found that just 5 per cent of employees think their organisation's cybersecurity culture is as advanced as it needs to be to protect their business from internal and external threats. More than 4,800 business and technology professionals shared their insights in the global research study, conducted via online polling in June 2018. Cybersecurity culture is a workplace culture in which security awareness and behaviors are seamlessly integrated into everyone's daily operations, as well as a strategic executive leadership priority. In a threat-ripe environment, an effective cybersecurity culture can help employees understand their roles and responsibilities in keeping their organisations safe and customer data secure. However, just 27 per cent of Oceania respondents (34 per cent of global respondents) say they understand their role in their organisations' cyber culture. Companies must take an all-hands-on-deck approach to counter cyberattack threats, the report summarises. "Enlisting the entire workforce to mitigate an enterprise's cyber risk is an emerging practice," says Doug Grindstaff II, SVP of Cybersecurity Solutions at CMMI Institute. "We are hearing a lot of feedback about how organisations can move the needle on employee involvement. It's challenging, but organisations are rightly concerned by the growing sophistication of cyberattacks." Widespread employee involvement correlates strongly with the minority of organisations that have achieved strong satisfaction with their cybersecurity culture. Nine in ten employees (92%) at these organisations say that their C-level executives share an excellent understanding of the underlying issues, which may be why they loop-in their employees so well; 84 per cent of employees at these organisations say they understand their role in cybersecurity. Other critical findings include: Many organisations lack the first—and all-important—step toward a cybersecurity culture: 57% of Oceania organisations (42% of global organisations) do not have an outlined cybersecurity culture management plan or policy. Aligning the entire workforce with the organisation's cybersecurity policies requires significant capital: Organisations that report a significant gap between their current and desired cybersecurity culture are spending just 19% of their annual cybersecurity budget on training and tools; organisations that believe their cybersecurity culture is where it is supposed to be are spending more than twice as much (43%). "A key motivator for organisations delaying investing in their cybersecurity cultures is a lack of awareness about the attempted threats and ongoing risks, as well as a lack of awareness about the assets at risk to cybersecurity threats," said Rob Clyde, CISM, NACD Board Leadership Fellow and ISACA Board Chair. "However, individuals tend to underestimate the potential damage and overestimate technology's ability to limit such incidents. Doing so puts their organisations at serious risk." To download the complimentary survey report, visit www.isaca.org/cybersecurity-culture-study. About ISACA Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organisations. ISACA leverages the expertise of its 450,000 engaged professionals in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including 217 chapters worldwide and offices in both the United States and China. Twitter: [www.twitter.com/ISACANews](https://twitter.com/ISACANews) LinkedIn: www.linkedin.com/company/isaca Facebook: www.facebook.com/ISACAHQ Instagram: www.instagram.com/isacanews/ About CMMI® Institute A subsidiary of ISACA Enterprises, CMMI Institute (cmmiinstitute.com) is the global leader in the advancement of best practices in people, process and technology. The Institute provides the tools and support for organisations to benchmark their capabilities and maturity by comparing their operations to best practices and identifying performance gaps. For over 25 years, thousands of high-performing organisations in a variety of industries, including aerospace, finance, healthcare, software, defense, transportation, and telecommunications, have improved their performance and earned a CMMI maturity level rating, and proved they are capable business partners and suppliers. Twitter: https://twitter.com/CMMI_Institute Contact: Julie Fenwick, +61 468 901 655 jfenwick@daylightagency.com.au Harriet Hall, +61 401 068 041, hhall@daylightagency.com.au

Contacts

Julie Fenwick
The Daylight Agency
mailto:
Niamh Hamill
0282357600
mailto:

Katya Ginsberg

8235 7600

mailto:

Karen Keech

0411 052 408

mailto:

Emma Catchpole

02 8235 7600

mailto: